8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,844	01/17/2001	Ronald P. Doyle	RSW920010007US1	6508

7590 03/02/2005

Jeanine S. Ray-Yarletts
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/764,844	**Applicant(s)** DOYLE ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2004* .

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-23,33,35-56 and 58-78* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-23,33,35-56 and 58-78* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 11/4/2004, applicant cancels claims 2, 24-32, 34, and 57 and amends claims 1, 8, 10, 13, 15, 16, 20, 33, 40-45, 47-53, 55-56, 63-65, 67-68, 70-76, and 78. The following claims 1, 3-23, 33, 35-56, and 58-78 are presented for examination.

2. The amendments to the specification, pages 2-4, filed on 11/4/2004 have been considered and the objection to the abstract has been withdrawn. Applicant has amended the specification to replace the "http://" with "www". The specification is still objected to because the format used for the hyperlinks is not an appropriate one in the amended specification as the hyperlinks "www" can still be executable. Applicant is suggested to place the hyperlinks in quotation marks. The objection to claims 10, 42, and 65, has been withdrawn with respect to the amended claims.

2.1 Applicant's arguments, pages 20-23, filed on 11/4/2004, with respect to the rejection of claims 1-78 have been fully considered, but they are not persuasive. Applicant has amended the independent claims to recite the step of "concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain connected until completion of the security-sensitive operation". Applicant argues that the step of concluding is not taught by Bjorn. However this added limitation is found in one of the cited art England (column 11, line 54 through column 12, line 8). Because the claims have been amended to further include the limitation of repeatedly accessing the stored secrets, the independent claims will be rejected in view of Matchett since Matchett discloses the added limitations. Therefore, applicant has not overcome the rejection of claim 1. The independent claims are now rejected in view of Bjorn and Matchett. The rejection of dependent claims not challenged by Applicant still apply in this office action.

Specification

3. The disclosure is objected to because it contains embedded hyperlinks and/or other form of browser-executable codes (see page 4, line 16; and page 29, line 7). Applicant is required to delete the embedded hyperlinks and/or other form of browser-executable codes. See MPEP § 608.01.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4.1 Claims 1, 33, 56, and 69, provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 26 of copending Application No. 09/764827. Although the conflicting claims are not identical, they are not patentably distinct from each other because the difference between the claims is that Application No. 09/764827 authenticating information using a biometric sensor, and the present application is using a card reader which would have been obvious to one skilled in the art because card reader, scanners, etc. are all biometric sensors and are well known in the art for obtaining biometric information.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 1, 3-4, 6, 7, 10, 13, 14, 16, 17, 19, 33, 35-36, 38, 39, 42, 45, 46, 48, 49, 51, 56, 58-59, 61, 62, 65, 68, 69, 71, 72, and 74** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,125,192 to **Bjorn et al.** in view of US Patent 5,229,764 to **Matchett et al.**.

5.2 **As per claims 1, 14, 33, 46, 56, and 69, Bjorn et al.** substantially teaches a method and system for providing continuous authentication of a user of a computing device, comprising: a security component which provides security functions, such that the security component can vouch for authenticity of one or more components with which it is securely operably connected, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27); a biometric sensor component that is securely operably connected as one of the one or more other components to the security component, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27 and column 4, line 39 through column 5, line 22); a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card, for example (see column 4, line 39 through column 5, line 22 and column 6, lines 18-27); a card reader for accessing the stored secrets and stored identifying information, for example (see column 4, line 39 through column 5, line 22); means for operably inserting the card into the card reader, for example (see column 16, lines 33-43); and means for establishing a secure operable connection between the biometric sensor, the card reader, and the security component, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27 and column 4, line 39 through column 5, line 22); means for obtaining from the biometric sensor component biometric input of a user of the computing device and means for comparing the obtained biometric input to the securely-stored biometric information of the authorized holder of the card, for example (see column 6, lines 27-43).

Matchett et al. in an analogous art teaches means for repeatedly obtaining from the biometric sensor component such as fingerprint sensor, retinal scan etc., for example (see column 1, lines 60 through column 2, line 3) biometric input of a user of the computing device and means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each comparison comprises an authentication of the user, for example (see column 3, lines 10-55). **Matchett et al.** discloses that if biometric checks are increased in duration and/or number, security would be enhanced and user substitution to an unauthorized user would be prevented, for example (see column 2, lines 55-66). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Bjorn et al.** to provide teaching means for repeatedly obtaining from the biometric sensor component biometric input of a user of the computing device and means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each comparison comprises an authentication of the user as taught by **Matchett et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Matchett et al.** so as to enhance security and prevent user substitution to an unauthorized user, for example (see column 2, lines 55-66).

Matchett et al discloses a continuous authentication by controlling any fraudulent including signal cut-off of the protected system during the continuous authentication (see an exemplary embodiment column 5, line 40 through column 6, line 28). Matchett discloses that in addition to a secure connection (column 9, lines 50 et seq.) security could be enhanced instructing the protected system or device to shut down should it be disconnected from the system 400 (column 10, lines 2-10). Figure 2 shows another secure configuration to protect "one or more systems or devices" column 8, lines 8-11 that meets the recitation of wherein the means for concluding that the security-sensitive operation is authentic also requires that all of the one or more components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain connected until completion of the security-sensitive operation, for example (see column 10, lines 3-5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Bjorn and Matchett to make determination that the secure-sensitive operation is authentic based on all of the one or more other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain connected until completion of the operation as suggested by **Matchett et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Matchett et al.** because keeping everything connected to monitor the use of the protected device is part of enhancing the security of a true continuous authentication (see column 4, line 55 through column 5, line 6, column 6, lines 10-26).

As per claims 16, 48, and 71, Bjorn et al discloses the limitation of wherein the stored identifying information comprises stored biometric information of the authorized holder, and further comprising means for comparing biometric information obtained with the biometric sensor from a user of the system, to the stored biometric information of the authorized holder, **Bjorn et al** also discloses wherein the means for comparing is performed by the biometric sensor, for example (see column 6, lines 27-43).

As per claims 3, 35, and 58, **Bjorn et al.** discloses the limitation of wherein selected ones of the secure operable connections are made using one or more buses of the security component, for example (see column 4, line 39 through column 5, line 22).

As per claims 4, 36, and 59, **Bjorn et al.** discloses the limitation of wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component, for example (see column 4, lines 18-22).

As per claims 6, 38, and 61, Bjorn et al. discloses the limitation of wherein selected ones of the secure operable connections are provided when the security component is manufactured, for example (see column 9, lines 52-62).

As per claims 7, 39, and 62, Bjorn et al. discloses the limitation of wherein the components comprise one or more of (1) input/output components and (2) application processing components, for example (see column 8, lines 4-30).

As per claims 10, 42, and 65, Bjorn et al. discloses the limitation of wherein the means for establishing a secure operable connection is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component, for example (see column 8, lines 4-30).

As per claims 13, 45, and 68, Bjorn et al. discloses the limitation of further comprising means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds, for example (see column 6, lines 27-43 and column 16, line 50 through column 17, line 5).

As per claims 17, 49, and 72, Bjorn et al. discloses the limitation of further comprising means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the means for comparing, for example (see column 6, lines 28-43 and column 17, lines 50-67).

As per claims 19, 51, and 74, Bjorn et al. discloses the limitation of wherein the means for comparing is performed by the security component, for example (see column 8, line 60 through column 9, line 3).

6. **Claims 5, 8, 9, 11, 12, 15, 18, 20, 21, 22, 23, 37, 40, 41, 43, 44, 47, 50, 52, 53, 54, 55, 60, 63, 64, 66, 67, 70, 73, 75, 76, 77, and 78** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,125,192 to **Bjorn et al.** in view of US Patent 5,229,764 to **Matchett et al.** as applied to claims 1, 33, 56, and 69 above, and further in view of US Patent 6,330,670 to **England et al.**.

6.1 **As per claims 5, 22, 37, 54, 60, and 77, Bjorn et al.** substantially teaches a method and system for securely providing biometric input from a user and means for securely operably connecting the biometric sensor the digital system that meets the recitation of the security component and the receiving unit that meets the recitation of the card reader. **Bjorn et al.** discloses an embodiment using a network, for example (see figure 3) and also discloses the sensor can be connected to a wireless system, or any indirect digital connection, for example (see column 4, lines 18-22). **Bjorn et al.** further discloses mutual authentication using public/private key and using a key each time a session is established and a timestamp to prevent stealing of the key, for example (see column 10, lines 1-22). It is very well known in the art wireless connection using SSL data encryption or equivalent that provides mutual authentication of both endpoints with a limited one-time key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system as combined above to provide wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key as suggested by **Bjorn et al.** to prevent stealing of the key for renegotiation.

England et al. in an analogous art teaches secure communication between components using SSL whereas keys are valid for a short period of time to prevent the key from being compromised, for example (see column 15, lines 29-45 and column 20, lines 40-57). **England et al.** also discloses a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is cryptographically-associated with the private cryptographic key, for example (see column 12, lines 53-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Bjorn et al.** to provide wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key as taught by **England et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **England et al.** so as to prevent the key from being compromised.

As per claims 8, 9, 11, 12, 21, 40, 41, 43, 44, 53, 63, 64, 66, 67, and 76, Bjorn et al. discloses the limitation of wherein the means for establishing a secure operable connection further comprises means for authenticating the biometric sensor to the security component and means for authenticating the security component to the biometric sensor, for example (see column 9, line 30 through column 10, line 7) and security handshake, for example (column 6, lines 52-65). **Bjorn et al.** discloses the limitation of wherein the means for authenticating the biometric sensor securely stored thereon. **Bjorn et al.** is silent about authenticating the card reader because of using an integral reader in its preferred embodiment, however, **Bjorn et al.** also discloses using a reader that can be attached to the security component through any connection, for example (see column 4, line 65 through column 5, line 6); when using an integral component, no duplicative memory, security units would be required otherwise strict security is necessary, for example (see column 5, lines 45-65). Therefore, one skilled in the art would be able to use disclosed by **Bjorn et al.** with a separate reader that will require the same authentication as the one for the sensor. It is apparent to one skilled in the art that one can mutually authenticate the card reader with the security component without departing from the scope and the spirit of the invention disclosed by **Bjorn et al.**.

England et al. in an analogous art also teaches mutual authentication of more than one component, for example (see column 12, lines 53-65) to provide a tamper resistant system. Therefore these claims are rejected on the same rationale as the rejection of claims 5, 37, and 60 above.

As per claims 15, 18, 47, 50, 70, and 73, Bjorn et al. discloses the limitation of wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising configured to digitally sign information presented to the card with the private key if the means for comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected, for example (see column 4, line 65 through column 5, line 6 and column 16, lines 32-

67). The authentication of the card reader was discussed above. Therefore these claims are rejected on the same rationale as the rejection of claims 5, 37, and 60. **Bjorn et al.** discloses a cross-authentication that would not be possible if the component is removed from the system (as mentioned in column 7, US Patent 6,577,733).

As per claims 20, 52, and 75, **Bjorn et al.** discloses the limitation of further comprising means for establishing a secure operable connection between an application processing component to the security component, and wherein the information presented to the card is generated by the established secure, operable connected application processing component, for example (see column 9, line 30 through column 10). **England et al.** also discloses application processing component to the security component to generate information from another component, for example (see column 12, lines 53-67). Therefore these claims are rejected on the same rationale as claims 5, 37, and 60.

Claims 23, 55, and 78 are similar to the rejected **claims 22, 54, and 77** except for incorporating the claimed method into a system. Therefore, **claims 23, 55, and 78** are rejected on the same rationale as the rejection of **claims 22, 54, and 77**.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin
Patent Examiner
February 21, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100